IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF TEXAS
DALLAS DIVISION

MELONIE PENRHYN, on behalf of Herself and all others similarly situated, ***Plaintiff,***	§	
vs.	§	**Civil Action No. 3:23-cv-2886**
NATIONSTAR FINANCIAL, INC. d/b/a MR. COOPER; and MR. COOPER GROUP, INC., ***Defendants.***	§	**COMPLAINT - CLASS ACTION** **JURY TRIAL DEMANDED**

COMPLAINT – CLASS ACTION

Plaintiff Melonie Penrhyn ("Plaintiff" or "Plaintiff Penrhyn"), individually on and on behalf of all similarly situated persons, by and through her undersigned counsel, files this Class Action Complaint against Nationstar Financial, Inc. d/b/a Mr. Cooper ("Nationstar"), and Mr. Cooper Group Inc., (collectively "Defendants" or "Mr. Cooper") and alleges the following based on personal knowledge of facts pertaining to her, on information and belief, and based on the investigation of counsel as to all other matters.

DESCRIPTION OF CASE

1. This class action arises out of the recent targeted cyber attack and data breach where unauthorized third-party criminals retrieved and exfiltrated personal data from Mr. Cooper's systems that resulted in unauthorized access to the highly sensitive data of Plaintiff, and according to Defendants, unauthorized access to the personally identifiable information ("PII") of all of its current and former customers – the individuals whose loans were serviced by Mr. Cooper.

2. As presented on its website, Mr. Cooper is the largest non-bank mortgage servicer in the country, with 6.5% of the market share.[1] As a mortgage servicer, Mr. Cooper is in possession of, and has a duty to protect, the PII of millions of consumers.

3. Despite its vast experience as a mortgage servicer to Americans, Mr. Cooper did not protect the PII of its customers – the Class Members.[2]

4. Stolen PII which includes social security numbers, financial and/or credit card payment account information – which are all at issue here – means and substantial risk of identity theft due to the breach. Freshly stolen information can be used with success against victims in specifically targeted efforts to commit identity theft known as social engineering or spear phishing. In these forms of attack, the criminal uses the previously obtained PII about the individual, such as name, address, email address, and affiliations, to gain trust and increase the likelihood that a victim will be deceived into providing the criminal with additional information.

5. Based on the value of its customers' PII to cybercriminals, Mr. Cooper knew or should have known the importance of safeguarding the PII entrusted to it and of the foreseeable consequences if its data security systems were breached. However, Mr. Cooper failed to take adequate cyber security measures to prevent the Data Breach from occurring.

6. Defendants maintained Class Members' Private Information in a negligent and/or reckless manner. In particular, the Private Information was maintained on Defendants' computer system and network in a condition vulnerable to cyber attacks. Upon information and belief, the mechanism of the cyber attack and potential for improper disclosure of Plaintiff's and Class

---

[1] *See* https://investors.mrcoopergroup.com/CorporateProfile/default.aspx, (last visited December 28, 2023).

[2] PII is referred to throughout this Complaint as "PII" or "Private Information" and contains information such as names, physical addresses, email addresses, phone numbers, dates of birth, Social Security numbers, bank account numbers, and taxpayer identification numbers.

Members' Private Information was a known risk to Defendants, and as such Defendants were on notice that failing to take steps necessary to secure Private Information from those risks left that Private Information in a vulnerable condition.

7. Armed with the Private Information accessed in the Data Breach, data thieves can commit a variety of crimes including opening new financial accounts and taking out loans in Class Members' names, using Class Members' names to obtain medical services (fraudulently implicating health insurance coverage benefits), using Class Members' Private Information to target other phishing and hacking intrusions based on their individual financial or health needs, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, and giving false information to police during an arrest.

8. On or around October 31, 2023, Mr. Cooper suffered a data breach in which an unauthorized third party obtained PII of some of its current and former customers ("Data Breach"). The cyber attack caused Mr. Cooper to shut down its technology systems preventing millions of borrowers from making payments on their loans between November 1, 2023, and November 4, 2023.[3]

9. Mr. Cooper's carelessness, negligence, and lack of oversight and supervision caused its customers to lose all sense of privacy. Plaintiff and members of the Class have suffered irreparable harm, including the exposure of their PII to nefarious strangers and their significantly increased risk of identity theft. The information at issue here is the very kind of information that allows identity thieves to construct false identities and invade all aspects of Plaintiff's and Class

[3] Mr. Cooper Group Inc., Form 8-K/A (Nov. 2, 2023, current report dated December 15, 2023) at https://investors.mrcoopergroup.com/financials/sec-filings/document-details/default.aspx?FilingId=17122632, (last visited December 28, 2023); Mr. Cooper Group December 15, 2023 Press Release, https://www.mrcoopergroup.com/press-releases/mr-cooper-group-update-on-recent-cyber-incident/ (last visited December 28, 2023).

members' lives. In addition to facing the emotional devastation of having such personal information fall into the wrong hands, Plaintiff and Class members must now undertake additional security measures and precautions to minimize their risk of identity theft.

10. Plaintiff's and the Class members' rights were disregarded by Mr. Cooper's negligent or reckless failure to take adequate and reasonable measures to ensure its data systems were secure and the PII entrusted to it would not be stolen. Mr. Cooper also failed to disclose the material fact that it did not have adequate information security controls to safeguard PII, failed to take foreseeable steps to prevent the Data Breach, and failed to monitor and timely detect the Data Breach.

11. As a result of the Data Breach, Plaintiff's and Class members' PII has been and will continue to be exposed to criminals for misuse.

12. Plaintiff brings this action individually and on behalf of the Class, seeking remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, injunctive relief, reasonable attorneys' fees and costs, and all other remedies this Court deems proper.

PARTIES

13. Plaintiff Penrhyn is currently a citizen and resident of the state of Florida as of 2021 and was previously a citizen and resident of New York. From approximately 2013 to August 2023, Nationstar and Mr. Cooper serviced Plaintiff Penrhyn's mortgage loan. This 2013–2023 time frame is during the duration of the Data Breach.

14. As Ms. Penrhyn's prior mortgage servicer, at the time of the Data Breach Mr. Cooper was in possession of her PII including but not limited to, her name, address, email

address, phone number, Social Security number, date of birth, and other confidential financial and credit information.

15. In its privacy policy, Mr. Cooper represented to Plaintiff and Class members that it is committed to respecting Plaintiff and Class members' data privacy, and that "[k]eeping financial information is one of our most important responsibilities. Only those persons who need it to perform their job responsibilities are authorized to access your information. We take commercially reasonable precautions to protect your information and limit disclosure by maintaining physical, electronic and procedural safeguards."[4]

16. Plaintiff and Class members did not initially choose to entrust their PII to Mr. Cooper directly, but instead their information was provided to Mr. Cooper because the servicing of their mortgage loan was transferred or sold to Mr. Cooper by the noteholder. Nevertheless, Plaintiff and Class members thereafter continued to supply Mr. Cooper with their PII because they understood from Mr. Cooper's representations, and duties as a mortgage servicer under the applicable law and regulations, that it would comply with its obligations to keep such information confidential and secure from unauthorized access, including thoroughly vetting all third parties it hired to ensured that they employed adequate data security measures, procedures, protocols, and practices.

17. Because of the Data Breach, Plaintiff's PII is now in the hands of criminals. Plaintiff and all Class members are now imminently at risk of crippling future identity theft and fraud.

18. Plaintiff Penrhyn did not receive any email or letter notice from Mr. Cooper about the cyber attack and data breach.

---

[4] *See* Mr. Cooper's Privacy Policy, https://www.mrcooper.com/privacy (last visited December 28, 2023).

19. After learning about the Mr. Cooper data breach through public reports and news covering the cyber attack, Plaintiff Penrhyn took affirmative action to take steps to mitigate the adverse consequences of the Data Breach, including reviewing account statements, monitoring credit reports, and changing passwords for all online accounts.[5]

20. As a direct and proximate result of the Data Breach, Plaintiff will need to continue purchasing a lifetime subscription for identity theft protection and credit monitoring.

21. Plaintiff has been careful to protect and monitor her identity. Plaintiff has also suffered injury directly and proximately caused by the Data Breach, including: (a) theft of Plaintiff's valuable PII; and (b) damages to and diminution in value of Plaintiff's PII that was entrusted to Defendants with the legal obligation to protect it; and (c) continued risk to Plaintiff's PII, which remains in the possession of Mr. Cooper (and now criminals) and which is subject to further breaches, so long as Mr. Cooper fails to undertake appropriate and adequate measures to protect the PII that was entrusted to Mr. Cooper.

22. Defendant Mr. Cooper Group Inc., formerly Nationstar Mortgage Holdings Inc., is a Delaware limited liability company with its principal place of business at 8950 Cypress Waters Boulevard, Coppell, Texas 75019.

23. Defendant Mr. Cooper is a Dallas-based mortgage lender and the largest non-bank mortgage servicer in the United States.[6]

JURISDICTION AND VENUE

24. Jurisdiction is proper in this Court under 28 U.S.C. § 1332 (diversity jurisdiction).

---

[5] *See*, for example, https://abcnews.go.com/Politics/mortgage-giant-mr-cooper-hit-cyberattack-possibly-affecting/story?id=105745061 (last visited December 29, 2023).

[6] https://www.forbes.com/advisor/mortgages/mr-cooper-mortgage-review/, (last viewed December 28, 2023).

Specifically, this Court has jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The claims alleged are on behalf of a class of consumers, there are more than 100 members of the proposed class, the amount in controversy exceeds $5 million, exclusive of interest and costs, and at least one Class Member is a citizen of a state different from Defendants.

25. Supplemental jurisdiction to adjudicate issues pertaining to state law is proper in this Court under 28 U.S.C. § 1367.

26. Defendants are headquartered and has its principal place of business of and/or routinely conducts business in the Dallas Division of the Northern District of Texas, has sufficient minimum contacts in the State of Texas, has intentionally availed itself of this jurisdiction by marketing and/or selling products and/or services and/or by accepting and processing payments for those products and/or services within the State of Texas.

27. Venue is proper in this District under 28 U.S.C. § 1391(a)(1) because a substantial part of the events that gave rise to Plaintiff's claims took place within the Dallas Division of the Northern District of Texas and Defendants are headquartered and/or have their principal place of business in the Dallas Division of the Northern District of Texas.

FACTUAL ALLEGATIONS

The Data Breach

28. On October 31, 2023, Mr. Cooper was the target of a cyber attack and data breach. In response, Mr. Cooper claims that it "took immediate steps to lock down"[7] its systems. Mr.

[7] *See* https://www.housingwire.com/articles/cyberattack-on-mr-cooper-forces-it-to-lock-down-systems/ (last visited December 29, 2023).

Cooper disclosed that this lock down prevented borrowers from being about to make payments or gain access to their account information for several days.[8]

29. On November 2, 2023, Mr. Cooper filed a Form 8-K with the United States Security and Exchange Commission ("SEC") disclosing the cyber attack. Mr. Cooper did not state in this filing whether any unauthorize disclosure of customer information had occurred. Mr. Cooper did state that it did not believe that the incident would have a material adverse effect on its business.[9]

30. On December 15, 2023, Mr. Cooper filed a supplemental report with the SEC, this time admitting that "personal information related to substantially all of our current and former customers was obtained from our system."[10] Mr. Cooper updated guidance for fourth quarter vendor expenses related to the cyber security incident to $25 million (from $5 to $10 million), which now includes an accrual for the cost of providing identify protection services for two years. Mr. Cooper made no change to its guidance for fourth quarter originations segment pretax operating earnings of $0 to $10 million and servicing segment pretax operating earnings of $200 to $210 million excluding MSR mark-to-market net of hedges.[11]

31. Mr. Cooper is responsible for allowing the Data Breach to occur because it failed to implement and maintain reasonable safeguards, failed to comply with industry-standard data security practices, as well as federal and state laws and regulations governing data security, and

---

[8] *See* https://www.securityweek.com/mortgage-giant-mr-cooper-shuts-down-systems-following-cyberattack/, (last visited December 28, 2023).
[9] *See* Mr. Cooper 8-K/A, (Nov. 2, 2023, current report dated December 15, 2023) at https://investors.mrcoopergroup.com/financials/sec-filings/document-details/default.aspx?FilingId=17122632, footnote number 1, *supra.*
[10] *Id.*
[11] *Id.*

failed to supervise, monitor, and oversee all third parties it hired who had access to Plaintiff's and the Class members' PII.

32. During the Data Breach, Mr. Cooper failed to adequately monitor its information technology infrastructure. Had Mr. Cooper done so, it would have prevented or mitigated the scope and impact of the Data Breach.

33. Plaintiff's and Class members' PII was provided to Mr. Cooper with the reasonable expectation and understanding that Mr. Cooper would comply with its obligations to keep such information confidential and secure from unauthorized access.

34. Mr. Cooper's data security obligations were particularly important given the substantial increase in cyber and ransomware attacks and data breaches in the financial services industries preceding the date of the Data Breach, as well as given the incredibly sensitive nature of PII that it retained in its servers.

35. By obtaining, collecting, and using Plaintiff's and Class members' PII, Mr. Cooper assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class members' PII from disclosure.

36. As a result of Mr. Cooper's failure to protect sensitive PII it was entrusted with, Plaintiff and Class members are at a significant risk of identity theft, financial fraud, and other identity-related fraud into the indefinite future. Plaintiff and Class members have also lost inherent value of their PII.

Mr. Cooper Was on Notice of Data Breach Threats and the Inadequacy of Its Data Security

37. Mr. Cooper's data security obligations were especially important given the substantial increase in cyber attacks and data breaches in recent years. In 2022, there were 1,802 reported data breaches, affecting approximately 422 million individuals.[12]

38. As Mr. Cooper boasts it is the "largest non-bank servicer with 6.5% of the market share" – thus an experienced financial services business -- Mr. Cooper's data security obligations were particularly important given the substantial increase in cyber attacks and/or data breaches in the financial industry, and other industries holding significant amounts of PII, preceding the date of the breach.[13]

39. At all relevant times, Defendants knew, or should have known that Plaintiff's and Class Members' Private Information was a target for malicious actors. Despite such knowledge, Defendants failed to implement and maintain reasonable and appropriate data privacy and security measures to protect Plaintiff's and Class Members' Private Information from cyber attacks that Defendants should have anticipated and guarded against.

40. Moreover, Defendants failed to implement and maintain reasonable and appropriate data privacy and security measures that would timely alert Defendants of any such attack, should one occur.

41. In light of recent high profile data breaches, Defendants knew or should have known that their electronic records and consumers' Private Information would be targeted by cybercriminals and ransomware attack groups.

---

[12] *See* https://www.idtheftcenter.org/wp-content/uploads/2023/01/ITRC_2022-Data-Breach-Report_Final-1.pdf, at page 2 (last visited December 28, 2023).

[13] *See* https://investors.mrcoopergroup.com/CorporateProfile/default.aspx (last visited December 29, 2023).

42. Mr. Cooper should have been aware—and was aware—that it was at risk of an internal data breach that could expose the PII that it collected and maintained.

43. Despite this, Mr. Cooper failed to take the necessary precautions required to safeguard Plaintiff's and Class members' PII from unauthorized access.

Mr. Cooper Failed to Comply with Statutory and Regulatory Obligations

44. Federal and State governments have established security standards and issued recommendations to minimize data breaches and the resulting harm to individuals and financial institutions. The Federal Trade Commission ("FTC") has issued numerous guides for businesses that highlight the importance of reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[14]

45. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which establishes guidelines for fundamental data security principles and practices for businesses.[15] Among other things, the guidelines note businesses should "Take Stock," "Scale Down," "Lock It," "Pitch It," and "Plan Ahead." In short, the guidelines explain that businesses should: (a) protect the sensitive consumer information that they keep; (b) properly dispose of PII that is no longer needed; (c) encrypt information stored on computer networks; (d) understand their network's vulnerabilities; and (e) implement policies to correct security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating

[14] *See Federal Trade Commission, "Start with Security: A Guide for Business"*, https://www.ftc.gov/system/files/documents/plain-language/pdf0205- startwithsecurity.pdf (last visited December 28, 2023).

[15] *See Federal Trade Commission, "Protecting Personal Information, A Guide for Business"* (October 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited December 28, 2023).

that someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[16]

46. Additionally, the FTC recommends that companies limit access to sensitive data, require complex passwords for network access, use industry-tested methods for security, monitor for suspicious activity on the network, and verify that third-party service providers have implemented reasonable security measures.[17]

47. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect PII, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

48. Mr. Cooper also failed to comply with commonly accepted industry standards for data security. Security standards commonly accepted among businesses that store PII using the internet include, without limitation:

- Design, maintain and test its computer systems, servers, and networks to ensure that all PII in its possession was adequately secured and protected;
- Maintain a secure firewall configuration;
- Maintain appropriate design, systems, and controls to limit user access or sharing of data to certain information as necessary;
- Monitor for suspicious or irregular traffic to servers in order to detect a breach of its data security systems in a timely manner;

[16] *Id.*
[17] *See* Federal Trade Commission, *"Start with Security: A Guide for Business,"* footnote 13, *supra*.

- Monitor for suspicious credentials used to access servers in order to detect a breach of its data security systems in a timely manner;
- Monitor for suspicious or irregular activity by known users in order to detect a breach of its data security systems in a timely manner;
- Monitor for suspicious or unknown users in order to detect a breach of its data security systems in a timely manner;
- Monitor for suspicious or irregular server requests in order to detect a breach of its data security systems in a timely manner;
- Monitor for server requests for PII;
- Monitor for server requests from VPNs; and
- Monitor for server requests from Tor exit nodes.

49. Mr. Cooper is also required by various states' laws and regulations to protect Plaintiff's and Class members' PII and to handle any breach of the same in accordance with applicable breach notification statutes.

50. In addition to its obligations under federal and state laws, Mr. Cooper owed a duty to Plaintiff and Class members whose PII were entrusted to Mr. Cooper to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Mr. Cooper owed a duty to Plaintiff and Class members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its systems and networks adequately protected the PII of Plaintiff and Class members.

51. Defendants owed a duty to Plaintiff and Class members whose PII was entrusted to Mr. Cooper to design, maintain, and test its systems to ensure that the PII in Mr. Cooper's possession was adequately secured and protected.

52. Mr. Cooper owed a duty to Plaintiff and Class members whose PII was entrusted to Mr. Cooper to create and implement reasonable data security practices and procedures to protect the PII in its possession.

53. Mr. Cooper owed a duty to Plaintiff and Class members whose PII was entrusted to Mr. Cooper to implement processes that would detect a breach on its data security systems in a timely manner.

54. Mr. Cooper owed a duty to Plaintiff and Class members whose PII was entrusted to Mr. Cooper to act upon data security warnings and alerts in a timely fashion.

55. Mr. Cooper owed a duty to Plaintiff and class members whose PII was entrusted to Mr. Cooper to disclose if its systems and data security practices were inadequate to safeguard individuals' PII from theft because such an inadequacy would be a material fact in the decision to entrust PII to Mr. Cooper.

56. Mr. Cooper owed a duty to Plaintiff and Class members whose PII was entrusted to Mr. Cooper to disclose in a timely and accurate manner when data breaches occurred.

57. Mr. Cooper owed a duty of care to Plaintiff and Class members because they were foreseeable and probable victims of any inadequacy in its affirmative development of the systems to maintain PII and in its affirmative maintenance of those systems.

58. In this case, Mr. Cooper was fully aware of its obligation to use reasonable measures to protect the PII of its customers. Mr. Cooper also knew it was a target for hackers. But despite understanding the consequences of inadequate data security, Mr. Cooper failed to comply with industry-standard data security requirements.

59. Mr. Cooper breached its obligations to Plaintiff and Class Members and/or were otherwise negligent and reckless because they failed to properly maintain and safeguard their

computer systems and data. Defendants' unlawful conduct includes, but is not limited to, the following acts and/or omissions based upon information and belief:

- Failing to maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;
- Failing to adequately protect customers' PII;
- Failing to properly monitor its own data security systems for existing intrusions;
- Failing to ensure that its vendors with access to its computer systems and data employed reasonable security procedures;
- Failing to train its employees in the proper handling of emails containing PII and maintain adequate email security practices;
- Failing to comply with FTC guidelines for cybersecurity, in violation of Section 5 of the FTC Act;
- Failing to adhere to industry standards for cybersecurity as discussed above; and
- Otherwise breaching its duties and obligations to protect Plaintiff's and Class Members' PII.

60. Defendants negligently and unlawfully failed to safeguard Plaintiff's and Class Members' PII by allowing cyberthieves to access their computer network and systems, which contained Private Information.

61. Accordingly, as set out in detail herein, Plaintiff and Class Members are exposed to an increased risk of fraud and identity theft.

The Effect of the Data Breach on Impacted Consumers

62. The exponential cost to Plaintiff and Class members resulting from the Data Breach cannot be overstated. Criminals can use victims' PII to open new financial accounts, incur charges in credit, obtain governmental benefits and identifications, fabricate identities, and

file fraudulent tax returns well before a person whose PII was stolen becomes aware of it.[18] Any one of these instances of identity theft can have devastating consequences for the victim, causing years of often irreversible damage to their credit scores, financial stability, and personal security.

63. Mr. Cooper was or should have been aware that it was collecting highly valuable data, which has increasingly been the target of data breaches in recent years.

64. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal PII to monetize the information. Criminals monetize the data by selling the stolen information on the black market to other criminals who then utilize the information to commit a variety of identity theft related crimes discussed below.

65. The exposure of any PII can cause unexpected harms one would not ordinarily associate with the type of information stolen. Cybercriminals routinely aggregate Private Information from multiple illicit sources and use stolen information to gather even more information through social engineering, credential stuffing, and other methods. The resulting complete dossiers of PII are particularly prized among cybercriminals because they expose the target to every manner of identity theft and fraud.

66. Identity thieves can use PII such as that exposed in the Data Breach to: (a) apply for credit cards or loans; (b) purchase prescription drugs or other medical services; (c) commit immigration fraud; (d) obtain a fraudulent driver's license or ID card in the victim's name; (e) obtain fraudulent government benefits or insurance benefits; (f) file a fraudulent tax return using

[18] Anita George, *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/,* (last accessed December 28, 2023); Brian Stack, *Here's How Much Your Personal Information Is Selling for on the Dark Web,* Experian, Dec. 6, 2017, https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/, (last accessed December 28, 2023); *In the Dark,* VPNOverview, 2019, https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/, (last accessed December 28, 2023).

the victim's information; (g) commit espionage; or (h) commit any number of other frauds, such as obtaining a job, procuring housing, or giving false information to police during an arrest.

Diminution of Value of PII

67. PII is valuable property and has been referred to as a "treasure trove for criminals."

68. PII's value is axiomatic, considering the value of Big Data in corporate America and that the consequences of cyber thefts include heavy prison sentences. Even this obvious risk-to-reward analysis illustrates, beyond doubt, that PII has considerable market value.

69. The PII stolen in the Data Breach is significantly more valuable than the loss of just credit card information in a large retailer data breach. Victims affected by those retailer breaches could avoid much of the potential future harm by simply cancelling credit or debit cards and obtaining replacements.

70. This type of data commands a much higher price on the dark web. As Martin Walter, senior director at cybersecurity firm RedSeal, explained: "Compared to credit card information, personally identifiable information … [is] worth more than 10x on the black market.[19] Sensitive PII, can sell for as much as $363 per record according to the Infosec Institute.[20]

[19] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT WORLD (Feb. 6, 2015), https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited Dec. 28, 2023).

[20] *See, e.g.*, John T. Soma, et al., *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("Private Information") Equals the "Value" of Financial Assets*, 15 RICH. J.L. & TECH. 11, at *3-4 (2009) ("Private Information, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

71. An active and robust legitimate marketplace for PII also exists. In 2019, the data brokering industry was worth roughly $200 billion.[21] Indeed, a Social Security number, date of birth, and full name can sell for $60 to $80 on the digital black market.[22]

72. As a result of the Data Breach, Plaintiff's and Class members' PII, which has an inherent market value in both legitimate and dark markets, have been damaged and diminished by its compromise and unauthorized release. However, this transfer of value occurred without any consideration paid to Plaintiff or Class members for their property, resulting in an economic loss. Moreover, the PII is now readily available, and the rarity of the data has been lost, thereby causing additional loss of value.

73. Plaintiff and Class members may not discover the fraudulent activity resulting from the Data Breach for years.

74. Plaintiff and Class members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. Plaintiff and Class members are incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

75. Mr. Cooper was, or should have been, fully aware of the unique type and the significant volume of data on Mr. Cooper's network, amounting to millions of individuals' detailed PII and thus the significant number of individuals who would be harmed by the exposure of the unencrypted data.

---

[21] David Lazarus, Column: *Shadowy data brokers make the most of their invisibility cloak*, L.A. TIMES (Nov. 5, 2019), https://www.latimes.com/business/story/2019-11-05/column-data-brokers (last visited December 28, 2023).

[22] Michael Kan, *Here's How Much Your Identity Goes for on the Dark Web*, PCMAG (Nov. 15, 2017), https://www.pcmag.com/news/heres-how-much-your-identity-goes-for-on-the-dark-web (last visited December 28, 2023).

76. The injuries to Plaintiff and Class members were directly and proximately caused by Mr. Cooper's failure to implement or maintain adequate data security measures for the PII of Plaintiff and Class members.

Loss of Time to Mitigate the Risk of Identity Theft and Fraud

77. As a result of the recognized risk of identity theft, when a data breach occurs and an individual is notified by a company that their PII was compromised, as in this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft of fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm.

78. Class members have spent, and will spend, time on a variety of prudent actions, such as researching and verifying the legitimacy of the Data Breach upon seeing news reports and monitoring their credit reports and financial accounts for suspicious activity.

79. The United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft face "substantial costs and time to repair the damage to their good name and credit record."[23]

80. These mitigation efforts are consistent with the 2007 Report from the U.S. Government Accountability Office regarding data breaches. Plaintiff's mitigation efforts are also consistent with the steps the FTC recommends data breach victims take to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to

[23] *See* U.S. Government Accountability Office, *"Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identify Theft is Limited; However, the Full Extent is Unknown,"* (Published June 4, 2007) (GAO-07-737), https://www.gao.gov/products/gao-07-737 (last visited December 28, 2023).

place a fraud alert (and considering an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[24]

81. Plaintiff and Class members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. Plaintiff and Class members are incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

82. Mr. Cooper was, or should have been, fully aware of the unique type and the significant volume of data on Mr. Cooper's network, amounting to millions of individuals' detailed PII and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

83. The injuries to Plaintiff and Class members were directly and proximately caused by Mr. Cooper's failure to implement or maintain adequate data security measures for the PII of Plaintiff and Class members.

Impact of Identity Theft Can Have Ripple Effects

84. Reimbursing a consumer for a financial loss due to fraud does not make that individual whole again. In addition to the irreparable damage that may result from the theft of a Social Security number, identity theft victims must spend numerous hours and their own money repairing the impact to their credit. The Department of Justice's Bureau of Justice Statistics found that identity theft victims "reported spending an average of about 7 hours clearing up the issues" and resolving the consequences of fraud in 2014.

[24] *See* Federal Trade Commission Consumer Advice, *"Identify Theft,"* https://consumer.ftc.gov/features/identity-theft, (last visited December 28, 2023).

85. The impact of identity theft can have ripple effects, which can adversely affect the future financial trajectories of victims' lives. For example, the Identity Theft Resource Center reports that respondents to their surveys in 2013-2016 described that the identity theft they experienced affected their ability to get credit cards and obtain loans such as student loans or mortgages.[25] For some victims, this could mean the difference between going to college or not, becoming a homeowner or not, or having to take out a high interest payday loan versus a lower-interest loan.

86. It is no wonder then that identity theft exacts a severe emotional toll on its victims.

87. Emotional Symptoms and Suffering. The 2017 Identity Theft Resource Center survey evidences the emotional suffering experienced by victims of identity theft:[26]

- 75% of respondents reported feeling severely distressed;
- 67% reported anxiety;
- 66% reported feelings of fear for the financial safety of family members;
- 24% reported fear for their physical safety;
- 15.2% reported that a relationship ended or was severely and negatively impacted by the identity theft; and
- 7% reported feeling suicidal.

88. Physical Symptoms and Suffering. Identity theft can also exact a physical toll on its victims. The same survey reported that respondents experienced physical symptoms stemming from their experience with identity theft:

- 48.3% of respondents reported sleep disturbances;

---

[25] *Identity Theft: The Aftermath 2017*, IDENTITY THEFT RES. CTR., https://www.idtheftcenter.org/post/the-identity-theft-resource-centers-2021-consumer-aftermath-report-reveals-impacts-on-covid-19-identity-crime-victims/, (last visited December 28, 2023).
[26] *Id.*

- 37.1% reported an inability to concentrate and/or lack of focus;
- 28.7% reported that they were unable to go to work because of physical symptoms;
- 23.1% reported new physical illnesses, including aches and pains, heart palpitations, sweating, and/or stomach issues;
- 12.6% reported a start or relapse into unhealthy or addictive behaviors.[27]

89. Time Lag. There may also be a significant time lag between when PII is stolen and when it is actually misused. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[28]

90. As the result of the Data Breach, Plaintiff and class members have suffered and/or will suffer or continue to suffer economic loss, a substantial risk of future identity theft, and other actual harm for which they are entitled to damages, including, but not limited to, the following:

- Losing the inherent value of their PII;
- Losing the value of Mr. Cooper's implicit promises of adequate data security;
- Identity theft and fraud resulting from the theft of their PII;
- Costs associated with the detection and prevention of identity theft and unauthorized use of their PII;

---

[27] *Id.*

[28] *See* U.S. Government Accountability Office, "Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identify Theft is Limited; However, the Full Extent is Unknown," (Published June 4, 2007) (GAO-07-737), footnote 22, *supra.*

- Costs associated with purchasing credit monitoring and identity theft protection services;

- Unauthorized charges and loss of use of and access to their financial account funds and costs associated with inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit;

- Lowered credit scores resulting from credit inquiries following fraudulent activities;

- Costs associated with time spent and the loss of productivity or the enjoyment of one's life from taking time to address and attempt to mitigate and address the actual and future consequences of the Data Breach, including discovering fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection services, imposing withdrawal and purchase limits on compromised accounts, and the stress, nuisance and annoyance of dealing with the repercussions of the Data Breach; and

- The continued imminent and certainly impending injury flowing from potential fraud and identify theft posed by their PII being in the possession of one or many unauthorized third parties.

91. Additionally, Plaintiff and Class members place significant value in data security.

92. Because of the value consumers place on data privacy and security, companies with robust data security practices can command higher prices than those who do not. Indeed, if consumers did not value their data security and privacy, companies like Mr. Cooper would have no reason to tout their data security efforts to their actual and potential customers.

93. Consequently, had consumers or noteholders known the truth about Mr. Cooper's data security practices—that Mr. Cooper would not adequately protect and store their data—the consumers' PII would not have entrusted to Mr. Cooper, or consumers would have purchased insurance to protect them from losses associated with Mr. Cooper's violative and negligent data security practices.

94. As such, Plaintiff and Class members did not receive the benefits and protection for to which they were entitled when their PII was entrusted to Mr. Cooper as their mortgage

servicer with the reasonable expectation that Mr. Cooper would adequately protect and store their sensitive personal and financial data. Mr. Cooper did not.

CLASS ACTION ALLEGATIONS

95. Plaintiff repeats and realleges each and every fact, matter, and allegation set forth above and incorporates them at this point by reference as though set forth in full.

96. Plaintiff brings this action on behalf of herself, individually, and on behalf of all other persons similarly situation ("the Class"), pursuant to Rule 23 of the Federal Rules of Civil Procedure.

97. Plaintiff seeks to represent a class of persons to be defined as follows, and proposes the following Class definition, subject to amendment as appropriate:

> **All persons in the United States and its territories whose personal identifiable information was compromised as a result of the Data Breach announced on or about November 2, 2023, (the "Nationwide Class").**

98. Excluded from the Class are Defendants' officers, directors, and employees, any entity in which Defendants have a controlling interest, and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of the Defendants. Also excluded from the Class are members of the judiciary to whom this case is assigned, their families and Members of their staff.

99. The proposed class definition is based on the information available to Plaintiff at this time.

100. Plaintiff reserves the right to amend or modify the Class definition or to create additional subclasses in an amended pleading or when she moves for class certification, as necessary to account for any newly learned or changed facts as the situation develops and discovery proceeds and as this case progresses.

101. ***Numerosity:*** Plaintiff is informed and believes, and thereon alleges, that the proposed Class is so numerous that joinder of all members is impracticable. Mr. Cooper services over 4 million mortgages meaning the total number of individuals affected in the Data Breach may be in the millions. The Members of the Class are so numerous that joinder of all of them is impracticable. Defendants acknowledged publicly that the PII of at most of its current and former customers was compromised in Data Breach.

102. ***Typicality:*** Plaintiff's claims are typical of the claims of the Class. Plaintiff and all members of the Class were injured through Mr. Cooper's uniform misconduct. The same event and conduct that gave rise to Plaintiff's claims are identical to those that give rise to the claims of every other Class member because Plaintiff and each member of the Class had their sensitive PII compromised in the same way by the same conduct of Mr. Cooper.

103. ***Adequacy***: Plaintiff is an adequate representative of the Class because Plaintiff's interests do not conflict with the interests of the Class; Plaintiff has retained competent counsel who are experienced in prosecuting complex class action and data breach class action litigation; and Plaintiff and Plaintiff's counsel intend to prosecute this action vigorously. The interests of the Class will be fairly and adequately protected by Plaintiff and her counsel.

104. ***Superiority:*** A class action is superior to all other available methods for the fair and efficient adjudication of this lawsuit because individual litigation of the claims of all members of the Class is economically unfeasible and procedurally impracticable. The injury suffered by each individual member of the Class is relatively small in comparison to the burden and expense of individual prosecution of litigation. It would be very difficult for members of the Class to effectively redress Mr. Cooper's wrongdoing. Further, individualized litigation presents a potential for inconsistent or contradictory judgments.

105. ***Commonality and Predominance:*** There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Defendants unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' Private Information;

b. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. Whether Defendants' data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

d. Whether Defendants' data security systems prior to and during the Data Breach were consistent with industry standards;

e. Whether Defendants owed a duty to Class Members to safeguard their Private Information;

f. Whether Defendants breached its duty to Class Members to safeguard their Private Information;

g. Whether Defendants knew or should have known that its data security systems and monitoring processes were deficient;

h. Whether Defendants exercised reasonable diligence in its monitoring and it should have discovered the Data Breach sooner;

i. Whether Plaintiff and Class Members suffered legally cognizable damages as a result of Defendants' misconduct;

j. Whether Defendants' conduct was negligent;

k. Whether Defendants breached implied contracts with Plaintiff and Class Members;

l. Whether Defendants was unjustly enriched by unlawfully retaining a benefit conferred upon them by Plaintiff and Class Members;

m. Whether Defendants failed to provide notice of the Data Breach in a timely manner, and;

n. Whether Plaintiff and Class Members are entitled to damages, civil penalties, punitive damages, treble damages, and/or injunctive relief.

106. ***Adequacy of Representation.*** Plaintiff is an adequate representative of the Class because her interests do not conflict with the interests of the Members of the Class. Plaintiff will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiff has retained Counsel who are competent and experienced in litigating class actions.

107. ***Predominance.*** Defendants have engaged in a common course of conduct toward Plaintiff and Class Members, similar or identical violations, business practices, and injuries are involved. Further, all the data of Plaintiff and Class Members was stored on the same computer system and unlawfully accessed in the same way. The common issues arising from Defendants' conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

108. ***Superiority.*** A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendants. In contrast, to conduct this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

109. ***Declaratory and Injunctive Relief Appropriate.*** Defendants have acted on grounds that apply generally to the Class as a whole, so that Class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

110. Likewise, particular issues under Rule 42(d)(l) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendants failed to timely notify the public of the Data Breach;

b. Whether Defendants owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their Private Information;

c. Whether Defendants' security measures to protect their data systems were reasonable in light of best practices recommended by data security experts;

d. Whether Defendants' failure to institute adequate protective security measures amounted to negligence;

e. Whether Defendants failed to take commercially reasonable steps to safeguard consumer PII; and

f. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

111. Finally, all members of the proposed Class are readily ascertainable. Defendants have access to Class Members' names and addresses affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by Defendants.

CAUSES OF ACTION

FIRST CAUSE OF ACTION
NEGLIGENCE
(*On Behalf of Plaintiff and the Nationwide Class)*

112. Plaintiff realleges and incorporates by reference Paragraphs 1 – 111 as if fully set forth herein.

113. By collecting and storing the PII of Plaintiff and Class Members, in their computer system and network, and sharing it and using it for commercial gain, Defendants owed a duty of care to Plaintiff and Class members to use reasonable means to secure and safeguard the entrusted PII, to prevent its unauthorized access and disclosure, to guard it from theft, and to detect any attempted or actual breach of its systems, as alleged herein. These common law duties existed because Plaintiff and Class members were the foreseeable and probable victims of any inadequate security practices in Defendants' affirmative development and maintenance of its data security systems and its hiring of third-party providers entrusted with accessing, storing, safeguarding, handling, collecting, and/or protecting Plaintiff's and Class members' PII. In fact, not only was it foreseeable that Defendants and Class members would be harmed by the failure to protect their PII because hackers routinely attempt to steal such information and use it for nefarious purposes, but Defendants also knew that it was more likely than not that Plaintiff and other Class members would be harmed by such exposure and theft of their PII.

114. Defendants owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that their systems and networks, and the personnel responsible for them, adequately protected the PII.

115. Plaintiff and Class Members are a well-defined, foreseeable, and probable group that Defendants was aware, or should have been aware, could be injured by inadequate data security measures.

116. Defendants' duties to use reasonable security measures also arose as a result of a special relationship with Plaintiff and Class members as a result of being entrusted with their PII, which provided an independent duty of care. Plaintiff's and Class members' PII was entrusted to Defendants predicated on the understanding that Defendants would take adequate security precautions. Moreover, Defendants were capable of protecting its network and systems, and the PII it stored on them, from unauthorized access.

117. In addition, Defendants had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

118. Defendants breached the aforementioned duties when it failed to use security practices that would protect the PII provided to it by Plaintiff and Class members, thus resulting in unauthorized exposure and access to Plaintiff's and Class members' PII.

119. Defendants further breached the aforementioned duties by failing to design, adopt, implement, control, manage, monitor, update, and audit its processes, controls, policies, procedures, and protocols to comply with the applicable laws and safeguard and protect Plaintiff's and Class members' PII within its possession, custody, and control.

120. As a direct and proximate cause of Defendants' failure to use appropriate security practices and failure to select a third-party provider with adequate data security measures,

Plaintiff's and Class members' PII was exposed, disseminated, and made available to unauthorized third parties.

121. Defendants admitted that Plaintiff's and Class members' PII was wrongfully disclosed as a result of the Data Breach.

122. The Data Breach caused direct and substantial damages to Plaintiff and Class members, as well as the likelihood of future and imminent harm through the dissemination of their PII and the greatly enhanced risk of credit fraud and identity theft.

123. By engaging in the foregoing acts and omissions, Defendants committed the common law tort of negligence.

124. Defendants breached its duties, and thus was negligent, by failing to use reasonable measures to protect Class Members' Private Information. The specific negligent acts and omissions committed by Defendants include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' PII;

b. Failing to adequately monitor the security of their networks and systems;

c. Failing to ensure that their email system had plans in place to maintain reasonable data security safeguards;

d. Failing to have in place appropriate mitigation policies and procedures;

e. Allowing unauthorized access to Class Members' PII;

f. Failing to detect in a timely manner that Class Members' PII had been compromised; and

g. Failing to timely notify Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

125. But for Defendants' wrongful and negligent breach of its duties owed to Plaintiff and Class members, their PII would not have been compromised.

126. Neither Plaintiff nor Class members contributed to the Data Breach or subsequent misuse of their PII as described in this Complaint.

127. As a direct and proximate result of Defendants' negligence, Plaintiff and Class members have been injured and are entitled to damages in an amount to be proven at trial. Such injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen PII; illegal sale of the compromised PII on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach investigating the nature of the Data Breach not fully disclosed by Defendants, reviewing bank statements, payment card statements, and credit reports; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the PII; lost benefit of their bargains and overcharges for services; and other economic and non-economic harm.

SECOND CAUSE OF ACTION
NEGLIGENCE *PER SE*
(*On Behalf of Plaintiff and the Nationwide Class*)

128. Plaintiff realleges and incorporates by reference Paragraphs 1 – 111 as if fully set forth herein.

129. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by Defendants of failing to use reasonable measures to protect PII. Various FTC publications and orders also form the basis of Defendants' duty.

130. Defendants violated Section 5 of the FTC Act (and similar state statutes) by failing to use reasonable measures to protect PII and not complying with industry standards. Defendants' conduct was particularly unreasonable given the nature and amount of PII obtained and stored and the foreseeable consequences of a data breach.

131. Defendants' violation of Section 5 of the FTC Act (and similar state statutes) constitutes negligence per se.

132. Plaintiff and Class members are consumers within the class of persons Section 5 of the FTC Act (and similar state statutes) were intended to protect.

133. Moreover, the harm that has occurred is the type of harm the FTC Act (and similar state statutes) was intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses which, as a result of Defendants failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiff and Class members.

134. As a direct and proximate result of Defendants' negligence, Plaintiff and Class members have been injured and are entitled to damages in an amount to be proven at trial. Such injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen PII; illegal sale of the compromised PII on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach investigating the nature of the Data Breach not fully disclosed by Defendants, reviewing bank statements, payment card statements, and credit reports; expenses and time spent

initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the PII; lost benefit of their bargains and overcharges for services; and other economic and non-economic harm.

THIRD CAUSE OF ACTION
BREACH OF IMPLIED CONTRACT
(*On Behalf of Plaintiff and the Nationwide Class)*

135. Plaintiff realleges and incorporates by reference Paragraphs 1 – 111 as if fully set forth herein.

136. Plaintiff and Class members entered into an implied contract with Defendants when they obtained products or services from Defendants, or otherwise provided PII to Defendants.

137. As part of these transactions, Defendants agreed to safeguard and protect the PII of Plaintiff and Class members and to timely and accurately notify them if their PII was breached or compromised.

138. Plaintiff and Class members entered into the implied contracts with the reasonable expectation that Defendants' data security practices and policies were reasonable and consistent with legal requirements and industry standards. Plaintiff and Class members believed that Defendants would use part of the monies retained by Defendants from their mortgage payments or the monies obtained from the benefits derived from the PII they provided to fund proper and reasonable data security practices.

139. Plaintiff and Class members would not have provided and entrusted their PII to Defendants in the absence of the implied contract or implied terms between them and Defendants. The safeguarding of the PII of Plaintiff and Class members was critical to realize the intent of the parties.

140. Plaintiff and Class members fully performed their obligations under the implied contracts with Defendants.

141. Defendants breached their implied contracts with Plaintiff and Class members to protect their PII when they (1) failed to take reasonable steps to use safe and secure systems to protect that information; and (2) disclosed that information to unauthorized third parties.

142. As a direct and proximate result of Defendants' breach of implied contract, Plaintiff and Class members have been injured and are entitled to damages in an amount to be proven at trial. Such injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen PII; illegal sale of the compromised PII on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach reviewing bank statements, credit card statements, and credit reports, among other related activities; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the PII; the amount of the actuarial present value of ongoing high-quality identity defense and credit monitoring services made necessary as mitigation measures because of Defendants' Data Breach; lost benefit of their bargains and overcharges for services or products; nominal and general damages; and other economic and non-economic harm.

FOURTH CAUSE OF ACTION
UNJUST ENRICHMENT
(In the alternative)
(*On Behalf of Plaintiff and the Nationwide Class)*

143. Plaintiff realleges and incorporates by reference Paragraphs 1 – 111 as if fully set forth herein.

144. This claim is pleaded in the alternative to the Breach of Implied contract claim set forth in the Third Cause of Action.

145. Plaintiff and Class members have an interest, both equitable and legal, in the PII about them that was conferred upon, collected by, and maintained by Defendants and that was ultimately stolen in the Data Breach.

146. Defendants benefitted from the conferral upon it of the PII pertaining to Plaintiff and Class members and by its ability to retain, use, sell, and profit from that information. Defendants understood that it was in fact so benefitted.

147. Defendants also understood and appreciated that the PII pertaining to Plaintiff and Class members was private and confidential and its value depended upon Defendants maintaining the privacy and confidentiality of that PII.

148. But for Defendants' willingness and commitment to maintain its privacy and confidentiality, Plaintiff and Class members nor any noteholder would not have provided Plaintiff and Class members' PII to Defendants or would not have permitted Defendants to gather additional PII.

149. Plaintiff's and Class members' PII has an independent value to Defendants.

150. Mr. Cooper admits that it uses the PII it collects for, among other things, providing consumers "opportunities to buy products" offered by itself or other financial institutions; sharing with other companies with which it has a joint marketing agreement; and tracking

consumers online activity across third-party websites and online services for the purpose of targeted advertising.[29]

151. Because of its use of Plaintiff's and Class members' PII, Defendants sold more services and products than it otherwise would have. Mr. Cooper was unjustly enriched by profiting from the additional services and products it was able to market, sell, and create through the use of Plaintiff's and Class members' PII to the detriment of Plaintiff and Class members.

152. Defendants also benefitted through its unjust conduct by retaining money paid by Plaintiff and Class members that it should have used to provide proper data security to protect Plaintiff's and Class members' PII.

153. It is inequitable for Defendants to retain these benefits.

154. As a result of Defendants' wrongful conduct as alleged in this Complaint (including among other things its failure to employ proper data security measures, its continued maintenance and use of the PII belonging to Plaintiff and Class members without having proper data security measures, and its other conduct facilitating the theft of that PII), Defendants have been unjustly enriched at the expense of, and to the detriment of, Plaintiff and Class members.

155. Defendants' unjust enrichment is traceable to, and resulted directly and proximately from, the conduct alleged herein, including the compiling and use of Plaintiff's and Class members' sensitive PII, while at the same time failing to maintain that information secure from intrusion and theft by hackers and identity thieves.

156. It is inequitable, unfair, and unjust for Defendants to retain these wrongfully obtained benefits. Defendants' retention of wrongfully obtained monies would violate fundamental principles of justice, equity, and good conscience.

---

[29] *See* Mr. Cooper Privacy Policy, footnote 4 *supra.*

157. The benefit conferred upon, received, and enjoyed by Defendants was not conferred officiously or gratuitously, and it would be inequitable, unfair, and unjust for Defendants to retain the benefit.

158. Defendants' defective security and its unfair and deceptive conduct have, among other things, caused Plaintiff and Class members to unfairly incur substantial time and/or costs to mitigate and monitor the use of their PII and has caused the Plaintiff and Class members other damages as described herein.

159. Plaintiff has no adequate remedy at law.

160. Defendants is therefore liable to Plaintiff and Class members for restitution or disgorgement in the amount of the benefit conferred on Defendants as a result of its wrongful conduct, including specifically: the value to Defendants of the PII that was stolen in the Data Breach; the profits Defendants received and is receiving from the use of that information; the amounts that Defendants overcharged Plaintiff and Class members for use of Defendants' products and services; and the amounts that Defendants should have spent to provide proper data security to protect Plaintiff's and Class members' PII.

FIFTH CAUSE OF ACTION
BREACH OF CONFIDENCE
(On Behalf of Plaintiff and the Nationwide Class)

161. Plaintiff realleges and incorporates by reference Paragraphs 1 – 111 as if fully set forth herein.

162. Plaintiff and Class members maintained a confidential relationship Defendants whereby Defendants undertook a duty not to disclose to unauthorized parties the PII that Plaintiff and Class members provide to Defendants. Such PII was confidential and novel, highly personal and sensitive, and not generally known.

163. Defendants knew Plaintiff's and Class members' PII was disclosed in confidence and understood the confidence was to be maintained, including by expressly and implicitly agreeing to protect the confidentiality and security of the PII it collected, stored, and maintained.

164. As a result of the Data Breach, there was an unauthorized disclosure of Plaintiff's and Class members' PII in violation of this understanding. The unauthorized disclosure occurred because Defendants failed to implement and maintain reasonable safeguards to protect the PII in its possession and failed to comply with industry-standard data security practices.

165. Plaintiff and Class members were harmed by way of an unconsented disclosure of their confidential information to an unauthorized third party.

166. But for Defendants' actions and inactions in violation of the parties' understanding of confidence, the PII of Plaintiff and Class members would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. Defendants' actions and inaction were the direct and legal cause of the theft of Plaintiff's and Class members' PII, as well as the resulting damages.

167. The injury and harm Plaintiff and Class members suffered was the reasonably foreseeable result of Defendants' unauthorized disclosure of Plaintiff's and Class members' PII.

168. Defendants knew their computer systems and technologies for accepting, securing, and storing Plaintiff's and Class members' PII had serious security vulnerabilities because Defendants failed to observe even basic information security practices or correct known security vulnerabilities.

169. As a direct and proximate result of Defendants' breach of confidence, Plaintiff and Class members have been injured and are entitled to damages in an amount to be proven at trial. Such injuries include one or more of the following: ongoing, imminent, certainly impending

threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen PII; illegal sale of the compromised PII on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach reviewing bank statements, credit card statements, and credit reports, among other related activities; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the PII; the amount of the actuarial present value of ongoing high-quality identity defense and credit monitoring services made necessary as mitigation measures because of Defendants' Data Breach; lost benefit of their bargains and overcharges for services or products; nominal and general damages; and other economic and non-economic harm.

By collecting and storing this PII and using it for commercial gain, Defendants have a duty of care to use reasonable means to secure and safeguard this PII to prevent disclosure and guard against theft of the PII.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff and the Class pray for judgment against Defendants as follows:

a. For an Order certifying this action as a Class action under Federal Rule of Civil Procedure 23, defining the Class as requested herein, appointing the undersigned as Class Counsel, and finding that Plaintiff Penrhyn is a proper representative of the Class requested herein;

b. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' Private Information, and from refusing to issue prompt, complete and accurate disclosures to Plaintiff and Class Members;

c. For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of Private Information compromised during the Data Breach;

d. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

e. Ordering Defendant to pay for not less than five years of credit monitoring and identify theft services for Plaintiff and the Class;

f. For injunctive and other equitable relief as necessary to protect the interests of Plaintiff and the Class as requested herein;

g. For an award of compensatory, consequential, and general damages, including nominal damages, as allowed by law in an amount to be determined;

h. For an award of restitution or disgorgement, in an amount to be determined;

i. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

j. For prejudgment interest on all amounts awarded; and

k. Such other and further relief as the Court may deem just and proper.

DEMAND FOR JULY TRIAL

Plaintiff demands a trial by jury on all triable issues.

Respectfully submitted,

/s/ *Kristina N. Kastl*
KRISTINA N. KASTL
State Bar No. 24025467
KASTL LAW, P.C.
4144 North Central Expressway, Suite 1000
Dallas, Texas 75204
(214) 821-0230
(214) 821-0231 Fax
kkastl@kastllaw.com
eservice@kastllaw.com

-AND-

ARIANA J. TADLER, ESQ. (*pro hac vice forthcoming*)
TONY K. KIM, ESQ. (*pro hac vice forthcoming*)
TADLER LAW, LLP

22 Bayview Avenue
Manhasset, New York 11030
(212) 946-9300
atadler@tadlerlaw.com
tkim@tadlerlaw.com

A.J. de BARTOLOMEO, ESQ. (*pro hac vice forthcoming*)
TADLER LAW, LLP
P.O. Box 475847
3749 Buchanan Street
San Francisco, CA 94123
(415) 226-0260
ajd@tadlerlaw.com

COUNSEL FOR PLAINTIFF PENRHYN AND THE PROPOSED CLASS